University of Michigan Press

Chapter Title: Political, Social, and Ethical Implications

Book Title: Fourth Revolution and the Bottom Four Billion
Book Subtitle: Making Technologies Work for the Poor
Book Author(s): Nir Kshetri
Published by: University of Michigan Press. (2023)
Stable URL: https://www.jstor.org/stable/10.3998/mpub.12205632.18

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at https://about.jstor.org/terms

This book is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0). To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/. Funding is provided by Knowledge Unlatched.

University of Michigan Press is collaborating with JSTOR to digitize, preserve and extend access to *Fourth Revolution and the Bottom Four Billion*

CHAPTER 11

Political, Social, and Ethical Implications

4R technologies have attracted growing political, social, and ethical attention. First, the importance of policy frameworks related to 4R technologies in economic and social development is being recognized. In 2019, a specialized technical committee on communication and information technologies of the African Union (AU), held in Sharm El Sheikh, Egypt, expressed the view that Africa's digital transformation depends on political commitment, appropriate policies and regulations, and the scaling up of investment and dedication of resources. The 2019 Sharm El Sheikh Declaration also emphasized the importance of the harmonization of legal and regulatory frameworks to create a single common digital market.[1]

A related point is that LMICs lag in terms of adequate legislation and enforcement to ensure responsible uses of 4R technologies such as AI and big data. In this regard, it is worth noting that in Europe, 96% of countries had data protection and privacy legislation in place as of October 2021 compared to 52% in Africa.[2] Of the world's 47 LDCs, only 21 (45%) had such legislation. LMICs that lack data protection laws are especially vulnerable to predatory and unethical practices of technology companies.

A related point is that some high-income countries are developing regulations to ensure that the uses of AI systems cause no harm to consumers. For instance, the European Commission released its proposed AI regulation on April 21, 2021.[3] The legislation included restrictions on facial recognition technologies.[4] Specifically, it prohibits the use of AI systems that cause or may cause "physical or psychological" harm through the use of "subliminal techniques" or by exploiting vulnerabilities of a "specific group of persons due to their age, physical or mental disability." It also bans AI systems from providing social scoring for use by public authorities, and it precludes the use of "real-time" remote biometric identification systems, such as facial recognition, in publicly accessible spaces for law enforcement purposes.[5] Most LMICs currently lack such initiatives.

---

[1] W. Gravett, "Digital neo-colonialism: The Chinese model of internet sovereignty in Africa," *African Human Rights Law Journal* 20, no. 1 (2020).

[2] UNCTAD, *Data protection and privacy legislation worldwide*, 2021, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[3] European Commission, *Proposal for a regulation on a European approach for artificial*

Second, there are a number of ethical issues associated with the 4R. A key ethical concern posed by the 4R, for instance, is related to collecting, storing, sharing, and accessing personal data. Technology startups desperately need more data. When companies gather an enormous amount of data, among the most pressing ethical issue is protecting people's privacy and empowering marginalized communities instead of exploiting them.[6] The hunger for data compounded by underdeveloped regulations and the lack of understanding of existing regulations to access personal information can lead to unethical data use.

It has been recognized that there is no easy short cut to developing and implementing ethical behavior in the AI industry in LMICs. At the First African Region Data Protection and Privacy International Conference organized by the UN Global Pulse, the Ministry of Communications for Ghana, and the Data Protection Commission for Ghana, participants noted that responsible and ethical AI practices require more than just laws. The key ingredients for such practices include increasing investment in AI education, educating technology-savvy lawyers and policymakers, and promoting gender equality in AI education.[7]

---

intelligence: Shaping Europe's digital future, August 24, 2022, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence.

[4] Madhumita Murgia, "Europe attempts to take leading role in regulating uses of AI," *Financial Times*, 2021, https://www.ft.com/content/360faa3e-4110-4f38-b618-dd695deece90.

[5] Mark MacCarthy and Kenneth Propp, "Machines learn that Brussels writes the rules: The EU's new AI regulation," *Brookings*, May 4, 2021, https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/.

[6] Karen Hao, "In 2020, let's stop AI ethics-washing and actually do something," *MIT Technology Review*, December 27, 2019, https://www.technologyreview.com/2019/12/27/57/ai-ethics-washing-time-to-act/.

[7] Mila Romanoff and P. Hidalgo-Sanchis, "Building ethical AI approaches in the African context," *UN Global Pulse*, August 28, 2019, https://www.unglobalpulse.org/2019/08/ethical-ai-approaches-in-the-african-context/.

Third, while many positive impacts of 4R technologies have been discussed in this book, these technologies also have important negative social impacts. For instance, issues such as AI bias affect some groups more than others. Some also argue that it is "overly simplistic" to describe this phenomenon as algorithm biased. They may be working as intended and predictions they make are accurate. The biases in AI could thus be the result of broader biases that exist in society.[8]

This chapter looks at the current stage of policies and regulations related to 4R technologies from the B4B populations' perspective. Social and ethical implications are also discussed.

National Policies, Regulations, and Enforcement

Broad Policy and Institutional Processes

Some countries have turned their attention to broad policy and institutional processes to benefit from the 4R. African economies such as Kenya, Tunisia, South Africa, Ghana, and Uganda are working to develop data protection and ethics strategies as a component of broader AI strategies and policies.[9] Many Latin American economies are also reported to be developing national AI plans[10]

In some economies, institutional capacity is being strengthened to benefit from the 4R. Rwanda's Centre for the Fourth Industrial Revolution brings together key stakeholders such as government agencies, the private sector, civil society, and academia. These actors work together to design, test, and refine policy frameworks and governance protocols to maximize the benefits of 4R technologies.[11] The center's main focus areas are AI and data policy.

---

[8] Will Knight, "AI programs are learning to exclude some African-American voices," *MIT Technology Review*, August 16, 2017, https://www.technologyreview.com/s/608619/ai-programs-are-learning-to-exclude-some-african-american-voices/.

[9] Romanoff and Hidalgo-Sanchis, "Building ethical AI approaches."

[10] Angelica Mari, "Artificial intelligence gathers pace in Latin America," *ZD Net*, June 11, 2020, https://www.zdnet.com/article/artificial-intelligence-gathers-pace-in-latin-america/.

[11] Julius Bizimungu, "Inside Rwanda's Centre for Fourth Industrial Revolution," *New Times*, November 25, 2020, https://www.newtimes.co.rw/news/inside-rwandas-centre-fourth-industrial-revolution.

Regulations Enabling the Use of 4R Technologies

Some LMICs have created regulations enabling the use of 4R technologies to bring economic and social transformation. For instance, in September 2019, a crop-spraying drone passed the South African Civil Aviation Authority (SACAA) regulations. Drones can spray in lands with challenging terrain that traditional aircraft cannot reach. They can also get closer to the crops, one to three meters above them, and programmed to follow mapped routes via GPS.[12]

Similarly, Zipline worked closely with policymakers in Ghana and Rwanda. Zipline reported that policymakers in the two countries were more willing to accommodate delivery drones in their airspace than the U.S., the EU, and other nations.[13]

The Center for the Fourth Industrial Revolution in San Francisco worked together with the Rwandan government to develop a regulatory framework for drone operations.[14] In 2016, the government of Rwanda approved regulations on drones, which made commercial drone delivery services for medical supplies possible.[15]

The government of Rwanda's policy frameworks around the use of drones is viewed as a model for other countries that want to use this technology. It is argued that developing countries, whose regulatory environments tend to be less robust than their developed country counterparts, can also be ideal places to test emerging technologies uses.[16]

---

[12] "South Africa's first crop-spraying drones can legally fly from today—saving farmers millions," *Farming Portal*, October 1, 2019, http://www.farmingportal.co.za/index.php/agri-index/74-tegnology/3155-south-africa-s-first-crop-spraying-drones-can-legally-fly-from-today-saving-farmers-millions.

[13] Faine Greenwood, "Assessing the impact of drones in the global COVID response," *Brookings*, July 30, 2021, https://www.brookings.edu/techstream/assessing-the-impact-of-drones-in-the-global-covid-response.

[14] Shusuke Murai, "New Tokyo research center aims to boost Japan's "Fourth Industrial Revolution," *Japan Times*, July 5, 2018, https://www.japantimes.co.jp/news/2018/07/05/business/tech/new-tokyo-research-center-aims-boost-japans-fourth-industrial-revolution/#.XaARbOMzaUk.

[15] Amar Toor, "This startup is using drones to deliver medicine in Rwanda," *Verge*, April 5, 2016, https://www.theverge.com/2016/4/5/11367274/zipline-drone-delivery-rwanda-medicine-blood.

[16] Catherine Cheney, "Rwanda could become a model for drone regulation," *Devex*, January 23, 2018, https://www.devex.com/news/rwanda-could-become-a-model-for-drone-regulation-91868.

Legislation on Responsible Use of 4R Technologies

Legislative measures are being put in place to control irresponsible and unethical business practices involving 4R technologies. One area has been the P2P lending industry. Digital P2P lenders allegedly charge high interest rates.[17] P2P lenders also harvest data from phones and used the data to embarrass debtors by calling family members.[18] The negative consequences of these practices disproportionately affect low-income people living in poverty.

Kenya is reported to have dozens of mobile phone microlenders such as the Silicon Valley–backed Tala that are not covered by the existing regulatory laws.[19] In August 2021, a parliamentary committee in Kenya backed a law to regulate digital lenders.[20] Likewise, Indonesia's Financial Services Authority (OJK) introduced draft proposals in 2020 to toughen existing rules by increasing paid-up capital requirements and mandating more frequent board meetings.[21]

Transforming the Government Sector

The 4R technologies can help governments in LMICs make intelligent decisions to benefit the poor and vulnerable groups. As discussed in chapter 6, remote-sensing technologies helped deliver vaccines, medical supplies, and equipment to remote areas in Ghana and Rwanda. The ultra-cold-chain technology needs a drop site of about two standard parking spaces. Big data can be used to improve existing services. For instance, in the education sector, data from devices, exams, and other sources can help design innovative ways to monitor student performance and improve teaching practices. Such tools can also be used in crime fighting and law enforcement. In Colombia's capital Bogotá, researchers are using big data to understand how crimes are related to public infrastructure such as bus stations, hospitals, schools, and drugstores.[22] Technologies such as blockchain can also help fight corruption in public procurement (In Focus 11.1)

---

[17] M. Ducan and M. Angus, "Kenyan parliamentary panel backs central bank to regulate digital lenders," *Reuters*, August 9, 2021, https://www.reuters.com/article/kenya-cenbank-idUSL8N2PG1TK.

[18] M. Ruehl, "Asian authorities clamp down on digital lenders," *Financial Times*, 2021, https://www.ft.com/content/b72c33a4-b6af-4a8d-8475-256fb7075546.

[19] Ducan and Angus, "Kenyan parliamentary."

[20] Ducan and Angus, "Kenyan parliamentary."

[21] Ruehl, "Asian authorities."

[22] World Bank, *Big data in action for government*: *Big data innovation in public services, policy and engagement*, 2017, https://documents1.worldbank.org/curated/en/176511491287380986/pdf/114011-BRI-3-4-2017-11-49-44-WGSBigDataGovernmentFinal.pdf.

In Focus 11.1: Blockchain in Colombia's School Meal Procurement

In Colombia, many corrupt practices have been reported in school meal procurement, and various scandals have arisen in recent years. The Colombian newspaper *El Tiempo* reported that that chicken breasts were sold to schools prices four times higher than local supermarkets.[23] In some cases, purchased goods are not delivered. The former mayor of the Caribbean port city Cartagena was charged for illegally contracting a deal of over COL$23 million (about US$7,000). Of 2.6 million purchased loaves of bread, 1 million were never delivered to schools. Public figures and officials and a small number of food contractors have been involved in procurement fraud.[24]

In an attempt to address corrupt practices in public procurement, the World Economic Forum teamed up with the Inter-American Development Bank (IDB) and the Office of the Inspector General of Colombia (Procuraduría General de Colombia) to investigate, design, and trial the use of blockchain for public procurement activities. A software proof-of-concept focused on a school meals program (Programa de Alimentación Escolar) for young people from low-income households was developed. A public blockchain procurement system was used to track the process of supplier selection in this program in the city of Medellín. Ethereum blockchain was used.[25]

The WEF's initial blockchain project in Colombia focused on contractor selection. The goal is to improve transparency, fairness, and competitiveness in a bidding process. A tenderer publicly commits to contract terms and selection criteria prior to eliciting bids. In this way, risks of favoring specific contractors are eliminated. For competing vendors, a blockchain-based solution's permanent and tamper-proof bid records can ensure that a firm cannot alter submitted bids after learning new information about competing bids. An additional benefit is that by increasing the perception of fairness, blockchain-led transparency can attract more vendors to the procurement process. A set of clearly defined selection criteria would increase the possibility that an outsider can win. During the auction and vendor evaluation processes, actions and decisions are automatically recorded. These records are permanent and publicly viewable, which increases auditability. It is also possible to include a user interface, which can be used by the public to monitor actions and decisions so that risks can be flagged in real time. These enable monitoring authorities such as the inspector general to investigate potential corrupt activity even before an auction concludes.

---

[23] "Una pechuga de pollo a $ 40.000 y huevo a $900, en sobrecostos del PAE," *El Tiempo*, 2017, https://www.eltiempo.com/justicia/investigacion/sobrecostos-en-programa-de-alimentacion-escolar-en-colombia-153590.

[24] M. Sarralde Duque, "En un año se robaron 32,8 millones de raciones de comida del PAE," *El Tiempo*, 2017, https://www.eltiempo.com/justicia/investigacion/desfalco-de-32-8-millones-en-raciones-de-comida-escolar-de-los-ninos-153928.

[25] I. Hall, "Colombian blockchain trial cause for 'cautious optimism,' says WEF," *Global Government Forum*, 2020, https://www.globalgovernmentforum.com/colombian-blockchain-trial-cause-for-cautious-optimism-says-wef/.

Blockchain-based solutions can also be used to monitor the chosen contractor's performance. For instance, information regarding actual deliveries can be made available to key stakeholders such as parents, teachers, enforcement officials, and the press. Their participants can be used to report meal deliveries and quality in real time. By improving observation in the delivery process and allowing stakeholders to monitor and engage, contractor accountability can be improved.[26] By allowing the participation of diverse groups, such systems can promote informal accountability, which, as prior research has shown,[27] can improve public procurement.

Efforts of Multilateral Organizations and Western Governments

Multilateral organizations, such as the African Development Bank and Western governments, have also provided support to undertake measures to strengthen national policies and strategies for utilizing 4R technologies and improving regulatory systems and enforcement measures. In March 2021, the African Development Bank approved a grant of US$1.024 million for AI to develop systems to process customer complaints on behalf of the national banks of Ghana and Rwanda and also Zambia's Competition and Consumer Protection Commission. The project aims to develop multilingual chatbots and artificial intelligence for financial regulators to handle complaints. It will incorporate key local languages for ease of use, record customer complaints, and track their resolution. Audio complaints will be used for those unable to read and write. The solution's deployment is planned in Kinyarwanda, Swahili, French, and English in Rwanda; English and Nyanja/Chewa in Zambia, and English and Twi in Ghana.[28] If successfully developed and deployed, the solution is likely to benefit linguistic minorities in these countries that are among the poorest groups.

---

[26] C. Barrera, S. Hurder, and A. Lannquist, "Here's how blockchain could stop corrupt officials from stealing school lunches," *World Economic Forum*, 2019, https://www.weforum.org/agenda/2019/05/heres-how-blockchain-stopped-corrupt-officials-stealing-school-dinners/.

[27] B. Romzek, K. LeRoux, and J. Blackmar, "A preliminary theory of informal accountability among network organizational actors," *Public Administration Review* 72, no. 3 (2012): 442–453.

International cooperation in law enforcement has also accelerated. The U.S. law enforcement authorities trained over 50 Nigerian investigators and prosecutors to handle cryptocurrency-enabled organized crimes. In August 2021, the International Computer Hacking & IP Attorney Advisers (ICHIP) in Addis Ababa, Ethiopia, and Abuja, Nigeria, and the Federal Bureau of Investigations (FBI) had organized a webinar focusing on cryptocurrency basics for investigators and prosecutors in Nigeria.[29]

Areas Needing Regulatory Attention

While recent developments on the policy and regulatory fronts are encouraging, some areas need regulatory attention. This section focuses on two key areas in which such attention is particularly needed.

Data Protection and Data Ownership Laws

Many people hold ill-informed or misguided views on the importance of data privacy for low-income people. Some argue that only wealthier and more privileged people need to worry about their privacy and have the ability to afford privacy- and security-enhancing measures such as encryption. It is argued that the digital divide has extended to become a "privacy divide."[30] For instance, one commentator noted that about 90% of the discussion at the 2013 internet Governance Forum (IGF) referred to big data as a surveillance tool. At the same time, the debate focusing on developing countries treated big data as a means to "observe" people to fight poverty. The argument provided by IGF participants was that data can help provide access to clean drinking water, healthcare, and other necessities.[31]

---

[28] Godfrey Ivudria, "$1 million for financial inclusion-African Development Bank," *EABW News*, March 10, 2021, https://www.busiweek.com/afdb-provides-1million-for-ai-ghana-rwanda-and-zambia/.

[29] Akon, "Akon: Why crypto could transform Africa's future," *Fortune*, April 14, 2021, https://fortune.com/2021/04/14/akon-city-senegal-africa-akoin-cryptocurrency.

[30] Jason Koebler, "Why mass surveillance is worse for poor people," *Motherboard*, February 24, 2015, http://motherboard.vice.com/read/why-mass-surveillance-is-worse-for-poor-people.

It might be argued that poor people need more—not less—privacy for their data. In countries where interethnic or tribal tensions and violence exist or where people live in the aftermath of a civil war, privacy is a genuine concern. Moreover, in countries characterized by conflict, crisis, and weak law enforcement, privacy breaches may lead to physical security risk.[32]

Of special concern is the data of 500 million smallholder farms worldwide, which employ more than 2 billion people. Such farms produce about 80% of food products consumed in Asia and SSA economies.[33] Farmers' personal data, such as demographic characteristics and household size, and crop and livestock farming data, such as land size, land ownership, average productivity and production value, number and value of inputs (e.g., seeds, fertilizers), livestock holding, and irrigation capability are highly valuable to businesses involved in the farm supply chain and financial institutions. Unsurprisingly, these data are highly sought after by the providers or technological solutions to farmers. For instance, the EcoProMIS project in Colombia (chapter 7) involves selling farming data to external partners, such as the service industry, government agencies, NGOs, and food processors.[34] Likewise, the Nigerian precision farming technology company Zenvus encourages farmers to share their farm data with banks to get loans. However, adequate protection of farmers' data is far from guaranteed.

To provide further insights into farmers' perceptions and responses to possible misuse of their farming data by various actors, it is important to contrast the situations in LMICs with those in high-income countries. In developed countries such as the U.S., farmers' awareness and activism is pushing the privacy agenda. Some farmers are concerned that big agricultural firms such as Monsanto might influence them to buy specific seeds, sprays, and equipment and be likely to profit from the costs of their services and higher seed sales.[35] Another key concern that farmers have expressed is that their data and information could be used by competitors. For example, other farmers' access to crop-yield information may create direct and unwanted competition to rent farmland, which may cause a new spike in land values and seed prices.[36] The issue regarding who owns farmers' crop data is of equal concern.[37]

---

[31] Linnet Taylor, *Surveil the rich, observe the poor: Big data at the Internet Governance Forum 2013*, October 25, 2013, http://linnettaylor.wordpress.com/2013/10/25/surveil-the-rich-observe-the-poor-big-data-at-the-internet-governance-forum-2013.

[32] E. Letouzé, "Big data for development: What may determine success or failure?" *OECD Technology Foresight*, Paris, 2012, https://www.oecd.org/sti/ieconomy/Session_5_Letouz%C3%A9.pdf.

[33] International Fund for Agricultural Development, *Enabling poor rural people to overcome poverty: Smallholders can feed the world*, 2011, https://www.ifad.org/documents/38714170/40706188/Smallholders+can+feed+the+world_e.pdf./460ca6c2-7621-40d8-9f79-a56f6f8fa75e.

[34] Agri-Innovation Den, *Meet our 2019 Agri-innovation Den Finalists*, 2019, https://www.aginnovationden.com/roelof-kramer-meet-our-2019-agri-innovation-den-finalists/.

Another fear is that Wall Street traders could use the data to make bets that hurt farmers. For instance, if conditions early in the growing season lead to lower futures contract prices, it may reduce the profits farmers could have made from crops.[38] Likewise, farmers are concerned that hedge funds or big companies might use real-time data at harvest time from many combines to speculate in commodities markets long before official crop-production estimates are available.[39] Such fears indeed rely on facts, as technology makes it possible to do so. For instance, a group at the MIT Media Lab used location data from mobile phones to estimate the number of people in Macy's parking lots on Black Friday. The model they developed made it possible to estimate the retailer's sales on that day even before Macy's had recorded sales. Insights like this are expected to provide competitive advantage to Wall Street analysts and managers.[40]

U.S. farmers also have raised additional concerns. For instance, if agriculture-related companies misuse or accidentally release their information, government auditors may scrutinize their finances or environmental activists may protest fertilizer and pesticide use.[41] However, such concerns have not yet been substantiated in LMICs.

Data security breaches in the U.S. have been eye-opening events for U.S.

---

35. T. J. Seppala, "Monsanto pushes big data-driven planting but farmers are skeptical," *Engadget*, February 26, 2014, https://www.engadget.com/2014-02-26-monsanto-prescriptive-farming.html.

36. Jacob Bunge, "Big data comes to the farm, sowing mistrust," *Wall Street Journal*, February 25, 2014, https://www.wsj.com/articles/SB10001424052702304450904579369283869192124.

37. Seppala, "Monsanto pushes."

38. Bunge, "Big data."

39. "American farmers confront big data revolution," *Fox News*, December 2, 2015, http://www.foxnews.com/us/2014/03/29/american-farmers-confront-big-data-revolution/.

40. Andrew McAfee and Erik Brynjolfsson, "Big data: The management revolution," *Harvard Business Review*, October 2012, http://hbr.org/2012/10/big-data-the-management-revolution/ar/1.

41. Shruti Singh and Jack Kaskey, "Farmers press agribusiness giants for data security," January 23, 2014, *Bloomber*g, https://www.bloomberg.com/news/articles/2014-01-23/farmers-press-agribusiness-giants-for-data-security.

farmers. In 2013, the Environmental Protection Agency, which gathers farm and livestock information to monitor air and water quality, inadvertently released to environmental groups personal information of 80,000 farmers.[42] Such events have provided the U.S. farmers with an environment to learn and become more familiar with data security and privacy issues. Such mechanisms are yet to evolve in many developing countries. Farmers in LMICs, who are often poor and less educated, often lack awareness and understanding of potential privacy and security risks.

Another challenge is related to data ownership. First, it is worth noting that in some advanced countries, insurers provide a high degree of privacy. For instance, in June 2019, the insurance firm Wakam (formerly La Parisienne Assurances) and Sigfox France announced a first usage-based insurance solution using connected objects, which focused initially on the mobility market (e.g., cars, motorcycles, electric scooters). It minimized data collection for General Data Protection Regulation (GDPR) compliance.[43]

Data misuse by service providers, third-party intermediaries, and other players is a concern due to underdeveloped data privacy regulations in LMICs. For instance, data created and made available through IoT makes it possible for insurers to better understand risk. The question is, Does the data belong to the insurance company or the customer? Customers may argue they have rights over their personal data. They might need access to historical data to switch insurers at renewal.[44] However, insurers may not give such data to consumers.

Regulations of Cryptocurrency Transactions

There has been a rapid rise in cryptocurrency transactions to facilitate business activities in LMICs. For instance, cryptocurrency transactions to and from Africa are primarily related to remittances and other legitimate business dealings.[45] As discussed in chapter 3, crypto-denominated international commerce has become increasingly common in LMICs.

---

[42] Singh and Kaskey, "Farmers press."

[43] Jorge Rudes, "La Parisienne Assurances automates contract management via the Quorum blockchain," *BitcoinDynamic*, April 6, 2020, https://bitcoindynamic.com/news/la-parisienne-assurances-automates-contract-management-via-the-quorum-blockchain/.

[44] SAS, *5 Challenges for IoT in the insurance industry*, 2019, https://www.sas.com/en_us/insights/articles/big-data/5-challenges-for-iot-in-insurance-industry.html.

[45] Richard Chelin, "Africa: new playground for crypto scams and money laundering—analysis," *Eurasia Review*, August 11, 2021, https://www.eurasiareview.com/11082021-africa-new-playground-for-crypto-scams-and-money-laundering-analysis/.

Some have developed innovative approaches based on blockchain that help employees receive faster payment from their employers. The Kenya-based blockchain startup BitPesa is helping speed the flow of cash from businesses in China to their African employees, who send money to their families. Launched in 2013, BitPesa uses bitcoin to facilitate low-cost instant payments.[46] As of the end of 2016, BitPesa operated in Kenya, Nigeria, Uganda, and Tanzania.[47]

It is important for governments in LMICs to ensure that crypto service providers have sufficient mechanisms in place to tackle money-laundering risks. Crypto businesses also should work with law enforcement to flag suspicious activities and help in the investigation.[48]

Digital Colonialism: Political and Social Consequences

It is argued that the operations of developed world technology companies competing for economic advantage in the cyberspace is akin to European colonial powers' competition over claiming the resources and control over colonies.[49] In this regard, it is helpful to begin by pointing to important political and social consequences of colonialism. For instance, colonialism involves political domination by colonialists, which leads to a significant reduction of the level of political sovereignty of the colonized. Likewise, "colonially-induced social transformation through immigration, proselytization and partition" has been reported in SSA economies.[50]

These long-standing concerns have been exacerbated by the activities of Chinese and Western technology firms in Africa and other LMICs. This phenomenon is often referred to as *digital colonialism*, defined as the "use of digital technology for political, economic and social domination of another nation or territory."[51] A primary goal of digital colonialism is data extraction.

---

[46] Malaka Gharib, "Blockchain could be a force for good. but first you have to understand it," *NPR*, January 11, 2017, http://www.npr.org/sections/goatsandsoda/2017/01/11/503159694/blockchain-could-be-a-force-for-good-but-first-you-have-to-understand-it.

[47] Zama Dyani, "Op ed: Africa needs more bitcoin and blockchain education," *Bitcoin Magazine*, December 20, 2016, https://bitcoinmagazine.com/articles/op-ed-africa-needs-more-bitcoin-and-blockchain-education-1482249305/.

[48] Chelin, "Africa."

[49] H. McClure, "Winter, the wild, wild web: The mythic American west and the electronic frontier," *Western Historical Quarterly* 31 (2000): 457–476.

[50] Patrick Ziltener and Daniel Künzler, "Impacts of colonialism: A research survey," *Journal of World-Systems Research* 19, no. 2 (2013): 290–311.

[51] Michael Kwet, "Long read digital colonialism," *New Frame*, March 8, 2021, https://www.newframe.com/long-read-digital-colonialism/.

To take an example, Berlin-based crypto startup Worldcoin uses metallic orbs to scan people's irises and collect other biometric data on faces and bodies. Worldcoin recruits country-level operators to collect biometric data. The operators receive commission in the stablecoin Tether for each person's biometric data that they collect. It conducted field testing mostly in LMICs such as Indonesia, Sudan, and Kenya. A civil engineer in Kenya's Nakuru city reported that he recruited between 150 and 200 people, at KES 50 (US$0.44) per scan. Likewise, in Indonesia's West Java province, an elementary school madrasa was used as a Worldcoin registration site to scan irises and other biometric data. The principal of the school was paid 2,000 Indonesian rupiah (IDR) ($0.14 US) for each person successfully scanned.[52]

In recent years, concerns have been mainly directed at Chinese and U.S. technology companies. In Africa, for instance, these technology companies frame their digital infrastructure projects as a humanitarian endeavor. Their ulterior motive, however, is arguably to extract data.[53] Their motivations are clear: the bigger and more diverse the dataset is, the more valuable the AI algorithm will be.

The Chinese Approach

Chinese AI corporations are leveraging global infrastructure projects initiated by the government, such as the Belt and Road Initiative, to secure contracts with African governments. In these deals, AI and other technology solutions are provided for free or at a low cost in exchange for access to local citizens' data. Chinese AI firms are relatively transparent about their goals. There is virtually no check or accountability as to how the information extracted from Africa will be used.[54]

To take an example, the Chinese company CloudWalk works with the Zimbabwean government to develop a facial recognition program. China described this as a "win-win" deal. Chinese AI companies can train ML algorithms on Africans to diversify their datasets, and Zimbabwe gets access to use the latest technology to monitor its population.[55]

---

[52] Eileen Guo and Adi Renaldi, "Deception, exploited workers, and free cash: How Worldcoin recruited its first half a million test users," *MIT Technology Review*, April 6, 2022, https://www.technologyreview.com/2022/04/06/1048981/worldcoin-cryptocurrency-biometrics-web3/.

[53] Nima Elmi, "Is big tech setting Africa back?," *Foreign Policy*, November 11, 2020, https://foreignpolicy.com/2020/11/11/is-big-tech-setting-africa-back/.

[54] Elmi, "Is big tech setting."

[55] "Exporting repression? China's artificial intelligence push into Africa," *Council on*

Regarding the motivation of Chinese technology companies' operations in Africa, the mass surveillance program implemented in Xinjiang has allowed Chinese companies to achieve some diversity in the data pool since the population of the province is mainly composed of Muslim Uyghurs, who are of Turkic descent.[56] But the datasets are still far from diverse enough. The CloudWalk deal in Zimbabwe provided access to a data pool with a much higher degree of diversity than China's ethnic composition can offer. It is the first Chinese AI project in Africa.

In terms of the upfront payment, it is possible that the Zimbabwean government paid for the technology and tools at a lower cost than it would have on the open market. However, CloudWalk received much more than monetary payment: data on the Zimbabwean people, which will provide the company an opportunity to improve its facial recognition systems. The Zimbabwean government failed to consider—or ignored—that high-dimensional biometric data such as faces are highly valuable. Natasha Msonza, cofounder of the Digital Society of Zimbabwe, noted: "It feels like [CloudWalk] is looking for guinea pigs. I don't believe that the Zimbabwe government gave this proposition much thought before volunteering its citizens to be subjected to racial facial recognition experiments."[57] Eric Olander, founder of the China Africa Project, noted that many Western companies "aren't willing to make that step that the Chinese are willing to do. . . . [The Chinese] are willing to make an investment in a market as volatile as Zimbabwe, where companies from other countries are not."[58]

In such a situation, what Gregory Unruh refers to as the techno-institutional complex (TIC) arises.[59] The idea is that radical systems such as those facilitated by the 4R should be viewed as a complex system of technologies embedded in a conditioning social context of public and private institutions. They should not be seen as a set of discrete technological artifacts.[60]

Foreign Relations, December 17, 2018, https://www.cfr.org/blog/exporting-repression-chinas-artificial-intelligence-push-africa.

[56] Amy Hawkins, "Beijing's big brother tech needs African faces. Zimbabwe is signing up for China's surveillance state, but its citizens will pay the price," *Foreign Policy*, July 24, 2018, https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/.

[57] Hawkins, "Beijing's big brother."

[58] Hawkins, "Beijing's big brother."

[59] Gregory C. Unruh, "Understanding carbon lock-in," *Energy Policy* 28 (2000): 817–830.

[60] Totti Konnola, Gregory C. Unruh, and Javier Carrillo-Hermosilla, "Prospective voluntary agreements for escaping techno-institutional lock-in," *Ecological Economics* 57, no. 2 (2006): 239–252.

The development of TIC takes place through a path-dependent, coevolutionary process. Such a process entails positive feedback among technological infrastructure and the organizations and institutions (e.g., regulatory agencies, and domestic and foreign creators) involved in creating and using them. Once countries and organizations are locked in, it becomes difficult to displace the existing system, which can lock out alternative technologies for a long period.[61]

To put things in context, in the long run, existing data projects increase Africa's dependence on China (and the West) and their technologies for policy formulation. For example, as Chinese firms accumulate data related to the movement of people and vehicles, African policymakers are more likely to rely on this private market information to develop solutions to infrastructure and transport problems.[62] African researchers referred to this as a form of digital neocolonization, similar to the exploitation of Africa by Western countries. China's "digital neocolonialism" in Africa arguably consists of three principal elements: promoting the Chinese model of internet sovereignty in African nations, exporting surveillance technologies that support authoritarian regimes, and deploying AI and data-mining techniques.

The Western (U.S.) Approach

Western corporations' approach is arguably more covert and embedded in seeming corporate social responsibility (CSR) activities. U.S. technology companies, for instance, are establishing digital hubs and providing free internet access. Some examples include Google's Internet Balloons and Facebook's Undersea Cable. It is argued that these initiatives "encourage more Africans to get online, use their services, and, by convenient coincidence, relinquish their data in the process."[63]

Some argue that through the domination of digital technology, the U.S. has reinvented colonialism in the Global South.[64] Commenting on U.S. technology companies' educational technologies in Brazil, Giselle Ferreira and her coauthors state that "when GAFA [Google, Amazon, Facebook, Apple] companies generously offer technologies to disadvantaged students, data is unimpededly extracted and subsequently treated in a manner that renders local specificities devoid of importance."[65]

---

[61] Konnola et al., "Prospective voluntary."

[62] Khwezi Nkwanyana, "China's AI deployment in Africa poses risks to security and sovereignty," *Strategist*, May 5, 2021, https://www.aspistrategist.org.au/chinas-ai-deployment-in-africa-poses-risks-to-security-and-sovereignty/.

[63] Elmi, "Is big tech setting."

[64] M. Kwet, "Digital colonialism: US empire and the new imperialism in the Global South," *Race & Class* 60, no. 4 (2019): 3–26.

To illustrate this, it is helpful to consider Google's approach. It is important to stress that Google's facial recognition project was alleged to be engaged in deceptive tactics targeting racial and ethnic minorities. Some of the contract workers, referred to by the company as temporary, vendor, and contractor (TVCs), which make up more than half of its total staff, were assigned to collect biometric data from minorities. They offered US$5 gift cards as incentive to collect face scans from minorities, which included homeless people in Atlanta, students in various universities, and attendees at the BET Awards event in Los Angeles.[66]

Tech companies such as Google lack access to data of diverse populations to realize the full benefits of AI-based facial recognition technology. One way to tackle this problem is to use the populations, such as those in Africa for data extraction. In 2019, Google opened an AI lab in Accra, Ghana.[67]

Some critics have questioned the motivation of Google's parent firm, Alphabet's Project Loon, which utilized a fleet of balloons to beam high-speed internet to some remote parts of the world. The project was shut down in early 2021. The defense company Raven Aerostar had built Google's balloons and flight-control systems. Raven Aerostar also manufactures balloons for the U.S. government's Columbia Scientific Balloon Facility, run by NASA. Raven Aerostar stated that its super-pressure balloons' "mission possibilities" include "scientific data collection, remote communications, GPS augmentation, intelligence gathering, persistent surveillance, reconnaissance, radar calibration, satellite simulation, incremental testing, and research and development of sensor."[68] The editor and wireless technology analyst Brad Reed at "Boy Genius Report" was quoted as saying: "If Google's claims about the Loon balloons' navigability are true, it is in fact an 'unmanned aircraft,' sometimes more pejoratively referred to as a drone. And what's worrisome is not so much Google's stated goal, but that with unprecedented proprietary technology, scant law on the books, and a few key government connections, Project Loon may only be a harbinger of a new era in our relationship to the skies overhead, one that our laws are dramatically unprepared for."[69] The editor and wireless technology analyst Brad Reed at "Boy Genius Report" was quoted as saying: "It's easy to understand why Google is working to bring mobile broadband connectivity to Africa: The company wants to get an early start on securing its next generation of customers."[70]

---

[65] G. M. dos S. Ferreira, L. A. da S. Rosado, M. S. Lemgruber, and J. de S. Carvalho, "Metaphors we're colonised by? The case of data-driven educational technologies in Brazil," *Learning, Media and Technology* 45, no. 1 (2019): 46–60.

[66] Ginger Adams Otis and Nancy Dillon, "Google using dubious tactics to target people with 'darker skin' in facial recognition project: sources," *Daily News*, October 2, 2019, https://www.nydailynews.com/news/national/ny-google-darker-skin-tones-facial-recognition-pixel-20191002-5vxpgowknffnvbmy5eg7epsf34-story.html.

[67] Kwasi Gyamfi Asiedu, "Google is throwing its weight behind artificial intelligence for Africa," *Quartz Africa*, June 14, 2018.

[68] Will K. Butler, "Can we trust Google with the stratosphere?," *The Atlantic*, August 20, 2013.

Another complaint is that Western technology companies are not providing their services to poor people who need them urgently. For instance, Loon had secured the government of Kenya's approval to launch balloons to provide commercial internet connectivity services. Some critics suggested that the balloons would have been better in another African country because Kenya already has an estimated 39 million out its 48 million people online.[71] Many technology companies want to extract as much valuable data as possible from their operations in LMICs.

U.S. technology companies have also been criticized for providing inferior products and services in LMICs. For instance, Facebook in India allegedly lacks key mechanisms to fight misinformation and hate speech that the company has deployed in the U.S. and other mostly-English-speaking countries for many years. For instance, Facebook had not developed algorithms to detect hate speech in Hindi and Bengali, the fourth and seventh most spoken languages in the world. It was also reported that some nefarious political actors had used multiple Facebook accounts to spread anti-Muslim messages across people's news feeds that clearly violated Facebook's rules.[72]

Government Surveillance and Espionage

Several counties are using 4R technologies to conduct surveillance activities on citizens. For instance, China is reported to have about 630 million

---

[69] "Google's plans to expand Internet access in Africa is about the data," *Deutsche Welle*, June 27, 2013, https://www.dw.com/en/googles-plans-to-expand-internet-access-in-africa-is-about-the-data/a-16903897.

[70] "Google's plans."

[71] "4G internet balloons take off over Kenya," *BBC News*, July 7, 2020, https://www.bbc.com/news/technology-53321007.

[72] Cat Zakrzewski, Gerrit De Vynck, Niha Masih, and Shibani Mahtani, "How Facebook neglected the rest of the world, fueling hate speech and violence in India," *Washington Post*, October 24, 2021, https://www.washingtonpost.com/technology/2021/10/24/india-facebook-misinformation-hate-speech/.

AI-based facial recognition cameras.[73] Chapter 9 discussed the Chinese government's, extensive surveillance mainly targeting the Uyghur community living in Xinjiang.

In the global debate over technology, the proliferation of AI-based surveillance systems and other aspects of exportable techno-authoritarianism have been among the major issues.[74] In recent years, China has exported AI-based surveillance to authoritarian markets and liberal democracies.[75]

Data and information services provider IHS Markit estimated that China accounted for nearly half the global facial recognition business in 2018.[76] Freedom House documented that 18 countries purchased AI surveillance tools from China in 2018:[77] These include Serbia,[78] Turkey, Russia, Ukraine, Azerbaijan, Angola, Laos, Kazakhstan, Kenya, Uganda,[79] Ecuador, Bolivia, and Peru.[80] Others suggest that only Huawei provides AI surveillance technology to at least 50 countries worldwide (In Focus: 11.2). No other company comes close.[81]

---

73. Anna Fifield, "Orwell's nightmare? Facial recognition for animals promises a farmyard revolution," *Washington Post*, August 24, 2020, https://www.washingtonpost.com/world/asia_pacific/facial-recognition-china-animals-farms-agriculture/2020/08/23/9808c710-d6fb-11ea-b9b2-1ea733b97910_story.html.

74. Andres Ortega, *The U.S.-China race and the fate of transatlantic relations, part 1: Tech, values, and competition*, Center for Strategic and International Studies, January 2020, http://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200113_USChinaTranstlanticRelations.pdf.

75. Steven Feldstein, "The global expansion of AI surveillance," *Carnegie Endowment for International Peace* September 2019, https://zhizhi88.com/wp-content/uploads/2019/10/2019%E5%B9%B4%E5%85%A8%E7%90%83%E4%BA%BA%E5%B7%A5%E6%99%BA%E8%83%BD%E7%9B%91%E6%B5%8B%EF%BC%88AIGS%EF%BC%89%E6%8C%87%E6%95%B0%E6%8A%A5%E5%91%8A.pdf.

76. Y. Yang, "Facial recognition: how China cornered the surveillance market," *Financial Times*, 2019, https://www.ft.com/content/6f1a8f48-1813-11ea-9ee4-11f260415385.

77. T. Mai, S. Adrian, W. Jessica, and F. Allie, *The rise of digital authoritarianism* (Freedom House, 2018), https://freedomhouse.org/sites/default/files/10192018_FINAL_FOTN_2018.pdf.

78. "Huawei's facial recognition technology causes anxiety in Serbia," *South China Morning Post*, October 17, 2019, https://www.scmp.com/news/world/europe/article/3033267/huaweis-facial-recognition-technology-causes-anxiety-serbia.

79. "Chinese facial recognition tech installed in nations vulnerable to abuse," *CBS News*, October 16, 2019, https://www.cbsnews.com/news/china-huawei-face-recognition-cameras-serbia-other-countries-questionable-human-rights-2019-10-16/.

80. Charles Rollet, "Ecuador's all-seeing eye is made in China," *Foreign Policy*, August 9, 2018, https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/.

81. Feldstein, "The global."

In Focus 11.2: Huawei's AI Surveillance

Privacy advocates are concerned about the potential misuse of data collected by AI-based surveillance systems provided by Chinese companies such as Huawei.[82] Deployment of China-developed solutions in countries with poor records on human rights is a concern.

In 2020, Ugandan police used Huawei's facial recognition systems to identify and arrest 836 suspected supporters of opposition leader Bobi Wine.[83] There is a lack of any judicial oversight and concerns of backdoor access to the system for illegal facial recognition surveillance. The system can be used to stifle anti-regime comments and peaceful civil action.[84] Through its Safe City projects, Huawei has supplied surveillance technologies to 16 African countries, often funded by China Exim Bank loans.[85]

The Philippine's Bonifacio Global City has been equipped with mass-surveillance systems developed by Huawei. The cameras are linked to data collection tools such as plate recognition. Huawei works with the police to fight crimes. It gathers evidence and identifies suspects using facial recognition technology.[86]

Nur Sultan, Kazakhstan, had over 2,000 cameras installed by Huawei working with Kazakhtelecom, Kcell, Beeline, and Tele2. The Tajikistan government implemented Huawei's "Safe Cities" system in Dushanbe in 2013. Over 800 cameras were reported to be watching monuments, parks, and other public spaces.[87]

---

82. Ben O'Rourke and Gigi Choy, "Big brother Huawei kitted out this Philippine city: Is China watching?," *South China Morning Post*, January 28, 2019, https://www.scmp.com/week-asia/economics/article/2183540/big-brother-huawei-watches-philippine-city-does-china-too.

83. "Three bodies of last week protests not claimed," *Monitor*, November 23, 2020, https://www.monitor.co.ug/uganda/news/national/three-bodies-of-last-week-protests-not-claimed-3207394.

84. Stephen Kafeero, "Uganda is using Huawei's facial recognition tech to crack down on dissent after protests," *Quartz*, November 27, 2020, https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters/.

85. Khwezi Nkwanyana, "China's AI deployment in Africa poses risks to security and sovereignty," *Australian Strategic Policy Institute*, May 5, 2021, https://www.aspistrategist.org.au/chinas-ai-deployment-in-africa-poses-risks-to-security-and-sovereignty/.

86. Nihrika Mandhana, "Huawei's video surveillance business hits snag in Philippines," *Wall Street Journal*, February 20, 2019, https://www.wsj.com/articles/huaweis-video-surveillance-business-hits-snag-in-philippines-11550683135.

87. Yau Tsz Yan, "Smart cities or surveillance? Huawei in Central Asia," *Diplomat*, August 7, 2019, https://thediplomat.com/2019/08/smart-cities-or-surveillance-huawei-in-central-asia/.

In December 2020, Myanmar rolled out the first phase of its "Safe City" initiative using a system of 335 surveillance cameras in eight townships in the capital, Naypyidaw.[88] In Myanmar, the launch of facial and license plate recognition was approved without public consultation or transparency. It is unclear how authorities plan to mitigate the technology's potential impact on human rights and the right to privacy.[89]

In Russia, rights groups say that migrants, particularly from Central Asia, are often subjected to racial profiling, arbitrary detention, and violence. The Russian IP video surveillance software company AxxonSoft's cameras have ethnicity analytics. The company said this feature was included in its product "inadvertently" when integrated with third-party software.[90]

Brazil is also allegedly sliding toward techno-authoritarianism.[91] In October 2019, then President Jair Bolsonaro signed a decree that requires all federal bodies to share their data they hold on Brazilian citizens, which will be consolidated in a centralized database. They include huge amounts of data, such as employment and health records, and biometric information such as face and voiceprint. While the government's stated goal is to use the data to improve public services and fight crimes, due to Bolsonaro's government's authoritarian path, critics have been concerned that the data may be used to spy on political dissidents[92]

---

[88] Thura Myat, "Nay Pyi Taw authorities activate 335 cameras able to detect faces," *Myanmar Times*, December 23, 2020, https://www.mmtimes.com/news/nay-pyi-taw-authorities-activate-335-cameras-able-detect-faces.html.

[89] "Myanmar: Facial recognition system threatens rights," *Human Rights Watch*, March 12, 2021, https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights.

[90] "'Racist' facial recognition sparks ethical concerns in Russia, analysts say," *Reuters*, July 5, 2021, https://www.voanews.com/europe/racist-facial-recognition-sparks-ethical-concerns-russia-analysts-say.

[91] Richard Kemeny, "Brazil is sliding into techno-authoritarianism," *MIT Technology Review*, August 19, 2020, https://www.technologyreview.com/2020/08/19/1007094/brazil-bolsonaro-data-privacy-cadastro-base/.

[92] "Podcast: COVID-19 is helping turn Brazil into a surveillance state," *MIT Technology Review*, September 16, 2020, https://www.technologyreview.com/2020/09/16/1008495/podcast-covid-19-brazil-surveillance-state/; Presidência da República Secretaria-Geral Subchefia para Assuntos Jurídicos Decreto Nº 10.046, October 9, 2019, http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm.

Ethics of Companies' Questionable Practices

Many companies are carrying out highly questionable practices from an ethical perspective. In this section, I illustrate some such practices.

Global Sweatshops

The emergence of global sweatshop factories of the 4R era has been a concern. One area that is especially important to consider is the data-labeling industry. The so-called ghost workers who do data annotation or labeling are distributed across the world.[93] They use online annotation platforms or work in annotation companies. In some cases, prisoners[94] and other economically vulnerable groups[95] do the labeling in jurisdictions that have limited labor laws. Some data-labeling firms have been accused of paying low wages. In this way, organizations engaged in this industry are allegedly facilitating a "new kind of slavery in the digital era."[96]

Although some data-labeling firms have claimed to produce positive social effects, such claims cannot be easily verified. There are virtually no regulations that govern the working conditions of data labelers. Industry standards related to ethical sourcing are weak. There is also a lack of third-party validation. We cannot thus really take self-reported information provided by these firms as proof that they are creating positive economic and social impacts in the developing world. There is little hard evidence to counter critics' concern that the firms claim that they engage impact sourcing is nothing more than marketing gimmicks or "impact washing."[97]

Another daunting challenge in getting data-labeling firms to engage in ethical practices is that the firms provide their services to businesses so face little public pressure. By contrast, fair-trade goods are directly sold to consumers.[98]

---

93. M. L. Gray and S. Suri, *Ghost work: How to stop Silicon Valley from building a new global underclass* (Eamon Dolan Books, 2019).

94. Karen Hao, "An AI startup has found a new source of cheap labor for training algorithms: prisoners," *MIT Technology Review*, March 29, 2019, https://www.technologyreview.com/f/613246/an-ai-startup-has-found-a-new-source-of-cheap-labor-for-training-algorithms/.

95. L. Yuan, "How cheap labor drives China's A.I. ambitions," *New York Times*, November 25, 2018.

96. Nicola Croce, "The new assembly lines: Why AI needs low-skilled workers too," *World Economic Forum*, August 12, 2019.

97. Kate Kaye, "These companies claim to provide 'fair-trade' data work. Do they?," *MIT Technology Review*, August 7, 2019.

98. Kaye, "These companies."

Some data-labeling firms, such as CloudFactory, DDD, iMerit, and Samasource, are members of the Global Impact Sourcing Coalition (GISC), founded in 2016. The GISC established an "impact sourcing standard" that defines minimum requirements and voluntary best practices for employment. The GISC requires member performance on criteria such as nondiscrimination and equal pay to be assessed every two years. Some well-known data-labeling firms such as Alegion are not GISC members.[99]

When it comes to promoting ethical and socially responsible behaviors, however, the GISC is at best of questionable effectiveness and value. For instance, violators face no penalty or sanction; they do not lose GISC membership. GISC members also differ significantly in the information they publish.

Samasource's impact audits report includes indicators such as workforce demographics and number of people lifted from poverty. DDD's reports contain information about employees' earnings and increase in lifetime income. CloudFactory had not published a social impact report since 2015. As of 2019, iMerit had not published any such reports[3]. The U.S.-based provider Alegion, which is not a GISC member, has outlined broad targets that it seeks to achieve but lacks specific metrics[3].

Moral Distance

Researchers have come up with the concept of moral distance, which refers to the use of data by organizations far from where it was collected.[100] For instance, human genome studies often ask participants to sign a form that gives them little direct control over the use of their data.[101]

There are concerns that international research-funding agencies and researchers from high-income economies set research priorities and establish data-sharing rules in Africa. Research participants in Africa are vulnerable to exploitation due to illiteracy and disease that are common in Africa. Also, many people have poor access to medical care. People participate in research to access doctors and other health professionals, when they are unwell.[102]

The argument is that if data is collected from an African village, the primary beneficiaries of that project should be the community in the village that serves as the data source. In most cases, the way data is collected and shared reflects the values and interests of organizations that are neither connected to nor have a vested interest in creating value for the communities providing the data. Many data initiatives in Africa are driven by well-intentioned efforts to fight against poverty and inequality. These initiatives, however, are driven by "deficit narratives," which means they focus on the continent's negative perception and ignore its positive contributions and assets. Data sharing is often inherently extractive. That is, data is collected from African communities without considering how communities where data is extracted from should be paid back. Data-sharing initiatives are mostly driven by non-African stakeholders. Data subjects themselves are not even viewed as stakeholders in the data-sharing process. There is also "data colonialism" where data of African communities is accessed and shared by heterogeneous geographies of people due to non-African organizations' unfair data-sharing practices. Local communities realize little benefits and are mostly harmed by these practices. Data sharing should be considered just like the farm-to-table movement, which involves growing and harvesting local ingredients and using them to serve meals to the local community. Data should contribute to fight poverty and help local communities rather than extract resources from them.[103]

---

[99] Kaye, "These companies."

[100] R. Abebe, K. Aruleba, A. Birhane, S. Kingsley, G. Obaido, S. L. Remy, and S. Sadagopan, "Narratives and counternarratives on data sharing in Africa," *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 2021.

[101] Linda Nordling, "Give African research participants more say in genomic data, say scientists," *Nature*, February 15, 2021, https://www.nature.com/articles/d41586-021-00400-9.

[102] Nordling, "Give African research."

Some initiatives are being taken to address the situation. In February 2021, the report Recommendations for Data and Biospecimen Governance in Africa was published by a committee of 13 African scientists.[104] The committee was formed by the African Academy of Sciences, based in Nairobi, and the African Union Development Agency, based in Addis Ababa, in June 2019. The report argues that the current way of data use can fuel distrust between researchers and participants, which needs to change.[105]

Workplace Surveillance

There has been a significant increase in workplace surveillance in recent years. It is argued that China's technology company workers are facing an environment similar to sweatshops. They work long hours to meet objectives set by big data analytics. They are constantly monitored, which, due to poor labor regulations, has created the potential for abuse.[106]

---

[103] Abebe et al., "Narratives and counternarratives."

[104] *Recommendations for data and biospecimen governance in Africa*, Alliance for Accelerating Excellence in Science in Africa, 2020, https://www.aasciences.africa/sites/default/files/Publications/Recommendations%20for%20Data%20and%20Biospecimen%20Governance%20in%20Africa.pdf.

[105] Nordling, "Give African research."

Adverse Social and Welfare Effects

Regarding the differential welfare effects on sophisticated and unsophisticated consumers, the median voter theory, developed and refined by Hotelling and others is of interest.[107,108] These authors specified the conditions and mechanisms under which competition between political parties would lead to an outcome that favors the median voter. Extending a median voter model in the context of big data, Strahilevitz predicted that the U.S. laws will "systematically favor the interests of sophisticated consumers, which are congruent with those of data miners, since sophisticated consumers are on the whole more politically engaged people who pay attention to legislative policy proposals and vote their interests."[109] Note that sophisticated consumers tend to be wealthier and better educated and have a higher tendency to vote. These consumers arguably think they will lose nothing from policies that allow firms to access their data,[110] and they are likely to make the necessary efforts to fight businesses' informational advantage. Some argue that the general public outside this group may not necessarily be a "winner" in economic or other terms in corporations' big data initiatives that rely on "data accessibility and manipulation."[111] Others maintain that gains associated with data-driven personalization primarily accrue to businesses that are resourceful and can see clear benefits of big data.[112]

Key aspects of the median voter theory can be extended to apply at the global level. A deduction from the median voter theory is that B4B populations face more adverse conditions for privacy protections. That is, they are more susceptible to privacy violations and face other social costs. 4R technologies are being used to exploit vulnerable populations in LMICs.

---

106. Nikki Sun, "China's tech workers pushed to their limits by surveillance software," *Financial Times*, June 15, 2021, https://www.ft.com/content/b74b6ad6-3b8d-4cd8-9dd6-3b49754aa1c7.

107. H. Hotelling, "Stability in competition," *Economic Journal* 39 (1929): 41–57.

108. B. A. Abrams and A. L. Kenneth, "A median-voter model of economic regulation," *Public Choice* 52 (1987): 125–142.

109. Strahilevitz, "Toward a positive theory."

110. Strahilevitz, "Toward a positive theory."

111. A. L. Allen, "Privacy law: Positive theory and normative practice," *Howard Law Journal* 56, no. 3 (2013): 241–251.

112. Aspen Institute, *The promise and peril of big data* (Queenstown, MD, 2010).

P2P Lenders and Fintech's Questionable Practices

P2P lenders and other fintech companies have engaged in unethical and questionable activities. In China, for instance, Ant Group uses its vast data and AI to analyze credit risk, which enabled the company to offer cheaper loans.[113] Ant Group and other Chinese fintech companies that use AI and big data analytics in extending loans are being accused of abusing personal data to collect debts. One such example is Ant Group's Ant Check Later, which allows users to delay payments and pay in installments. An online user reported being contacted by Ant Check Later for information about a friend who owed money to the payment service. Ant Group reportedly said that the practice of contacting a borrower's friends or relatives to help with collecting debts is common in the financial sector. TMTpost cited a China Youth Daily poll, which showed that 76% of respondents believed there was data abuse.[114] Users of JD.com reported similar problems. The JD.com financial unit operates JD Baitiao, similar to Ant Check Later. In a question posted on the online legal advice site 110.com, a JD.com user asked if it was legal for JD.com to give a third-party service his personal information for the purpose of debt collection. Fintech companies in Kenya are also reported to use "societal shaming" for debt collection.[115]

Customers have reported that friends and family were harassed after they were late in repaying loans offered by Silicon Valley–based personal credit startups in Kenya. Debt shaming has led to at least one suicide in Kenya.[116] A January 2021 *Wired* article reported that at least eight people in India who had been the victims of harassment by quick loan apps had committed suicide in the previous two months.[117] In China, it has been reported that many women were required to share their nude pictures as collateral. In 2016, a student from Jiangsu Province reported that she agreed to provide nude photos to private lenders in exchange for a loan of 120,000 RMB (US$18,781) to start a small business.[118]

---

[113] Gillian Tett, "Artificial intelligence is reshaping finance," *Financial Times*, November 19, 2020, https://www.ft.com/content/c7d9a81c-e6a3-4f37-bbfd-71dcefda3739.

[114] "Online credit services in China accused of abusing personal data," *Want China Times*, 2015, www.wantchinatimes.com/news/content?id=20150927000087&cid=1203.

[115] Olumuyiwa Olowogboyega, "Countdown: The 10 most important African tech companies of the decade," *Techcabal*, December 26, 2019, https://techcabal.com/2019/12/26/countdown-the-10-most-important-african-tech-companies-of-the-decade/.

[116] Antoaneta Roussi, "Kenyan borrowers shamed by debt collectors chasing Silicon Valley loans: Customers say friends and family were harassed after they were late repaying US startup branch," *Financial Times*, September 9, 2020, https://www.ft.com/content/16c86479-e88d-4a28-8fa4-cd72bace5104.

[117] Varsha Bansal, "Shame, suicide and the dodgy loan apps plaguing Google's Play Store," *Wired*, January 20, 2021, https://www.wired.co.uk/article/google-loan-apps-india-deaths.

Global and Regional Norms

It is important to look at the role and importance of global norms in influencing the use of 4R technologies. For instance, global and national money-laundering regulations including customer due diligence, reporting of suspicious transactions, and record keeping are needed to increase the adoption of payment systems such as cryptocurrencies.[119]

A complaint that is often heard is that developed countries are disproportionately benefiting from global norms, which are being shaped to benefit them. LMICs arguably have not been given an opportunity to participate in discussions involving global AI governance.[120] LMICs are highly underrepresented in international AI advisory boards, expert panels, and councils appointed by international organizations, which has resulted in the lack of regional diversity. This underrepresentation in AI governance can be attributed to geopolitical power imbalances of the colonial era.[121] For instance, in the UNICEF's AI for Children project's expert advisory group, there are no representatives from regions that have the highest concentration of children and young adults, including the Middle East, Africa, and Asia.[122]

Some have refused to participate in international data agreements.[123] In the 2019 G20 Summit held in Japan, India did not sign the Osaka Track declaration, launched by Japan's then prime minister Shinzo Abe to promote cross-border data flow.[124]

---

[118] Stuart Leavenworth, "China's 'naked loans' force female students to bare all in return for more cash," *The Guardian*, June 15, 2016, https://www.theguardian.com/world/2016/jun/15/chinas-naked-loans-force-female-students-to-bare-all-in-return-for-more-cash.

[119] Richard Chelin, "Africa: New playground for crypto scams and money laundering—analysis," *Eurasia Review*, August 11, 2021, https://www.eurasiareview.com/11082021-africa-new-playground-for-crypto-scams-and-money-laundering-analysis/.

[120] Hao, "The problems AI."

[121] Hao, "The problems AI."

[122] Abhishek Gupta and Victoria Heath, "AI ethics groups are repeating one of society's classic mistakes," *MIT Technology Review*, September 14, 2020, https://www.technologyreview.com/2020/09/14/1008323/ai-ethics-representation-artificial-intelligence-opinion/.

[123] Hao, "The problems AI."

The dominance of the EU and other developed economies in the development of global AI governance and ethical frameworks has been a concern for LMICs that lack institutional capacity. For instance, it is argued that such frameworks are harder to adhere to for Latin American companies. Since the EU has stricter regulations, it could hamper the development of the Latin American AI industry. It is argued that while countries such as Japan, despite having different regulatory regimes, have negotiated agreements with the EU, Latin America lacks such negotiating strength.[125]

The global AI ecosystem can also benefit from regional collaboration. For instance, it is argued that due to the disjointed regulatory and policy environment, countries in Latin America lack a unified voice on this issue.[126]

Chapter Summary and Conclusion

The discussion in this chapter makes it clear that the 4R has important political, social, and ethical dimensions that policymakers, businesses, consumers, and other actors should consider. It is encouraging that new regulations are being enacted in some LMICs to benefit from the 4R. Some countries are also putting in place legislative measures to control irresponsible and unethical business acts utilizing 4R technologies.

Nonetheless, there is a divergence between LMICs and high-income economies in some key regulatory areas related to the 4R. Weak and underdeveloped regulatory environments in many LMICs have facilitated the misuse and abuse of personal data. Poor people's lack of capability and resources to defend themselves would make data privacy more—not less—important for them. Due to such environments, in many cases, big technology companies are enriching themselves using data obtained from low-income people and small businesses. In some cases, these companies' activities bring little or no benefits to these vulnerable groups. A related point is that some uses of 4R technologies have adverse welfare effects on unsophisticated consumers. A core concern is that there is a relative lack of voice and representation of the B4B in the global AI industry.

---

[124] Ankur Taliyan, "G20 Summit: Why India refused to sign Osaka declaration on global data flow," *Times Now News*, July 4, 2019, https://www.timesnownews.com/india/article/g20-summit-why-india-refused-to-sign-osaka-declaration-on-global-data-flow/446887.

[125] "The global AI agenda: Latin America," *MIT Technology Review*, 2020, https://mittrinsights.s3.amazonaws.com/AIagenda2020/LatAmAIagenda.pdf.

[126] Angelica Mari, "Artificial intelligence gathers pace in Latin America," *ZD Net*, June 11, 2020, https://www.zdnet.com/article/artificial-intelligence-gathers-pace-in-latin-america/.

Some governments have identified an opportunity to use data to achieve their political agenda. Surveillance and espionage have also increased because 4R technologies have greatly increased the ease with which these activities can be performed. They are misusing 4R technology to conduct espionage on citizens and engage in activities that violate their privacy and human rights. These concerns have been especially strongly voiced against countries that have used China-developed solutions. This chapter also illustrated businesses' certain questionable practices related to the uses of 4R technologies from an ethical perspective.

This chapter has provided an account of how LMICs are playing key roles in the global AI industry: However, due to global technology companies' practices of ethics dumping and ethics shirking, minimal benefits have been observed in LMICs. Many companies are going for a data grab under cover of helping poor and marginalized groups. Currently, the nascent technology industries of most developing countries cannot compete globally with those from China or the U.S. However, companies from China and the U.S. can maintain control over local policies.